

INTERNATIONAL SEARCH REPORT

International Application No
PCT/JP2004/005528

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>J. SILVERMAN: "WRAPS, GAPS, AND LATTICE CONSTANTS" NTRU CRYPTOSYSTEMS TECHNICAL REPORT, REPORT 11, 'Online! 15 March 2001 (2001-03-15), pages 1-6, XP002288211 Retrieved from the Internet: URL: http://www.ntru.com/cryptolab/pdf/NTRU_Tech011_v2.pdf 'retrieved on 2004-07-12! cited in the application the whole document</p> <p style="text-align: center;">----- -/--</p>	1-37

☒ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

14 July 2004

Date of mailing of the international search report

06/08/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Bec, T

INTERNATIONAL SEARCH REPORT

International Application No
PCT/JP2004/005528

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	J.H. SILVERMAN, W. WHYTE: "estimating decryption failure probabilities for nrtuencrypt" NTRU CRYPTOSYSTEMS TECHNICAL REPORT 18, 'Online! June 2003 (2003-06), pages 1-17, XP002288212 Retrieved from the Internet: URL:http://www.ntru.com/cryptolab/pdf/NTRU Tech018.pdf> 'retrieved on 2004-07-12! the whole document	1-37
X,P	N. HOWGRAVE-GRAHAM, P.Q NGUYEN, D.POINTCHEVAL, J. PROOS, J.SILVERMAN, A.SINGER, W. WHYTE: "THE IMPACT OF DECRYPTION FAILURES ON THE SECURITY OF THE NTRU ENCRYPTION" IN PROC. CRYPTO 2003, SANTA BARBARA, USA, 2003, 'Online! August 2004 (2004-08), pages 1-22, XP002288213 Retrieved from the Internet: URL:http://www.ntru.com/cryptolab/pdf/cr03 _ntru.pdf> 'retrieved on 2004-07-12! the whole document	1-37
A	J.H SILVERMAN: "DIMENSION-REDUCED LATTICES ZERO-FORCED LATTICES AND THE NTRU PUBLIC KEY CRYPTOSYSTEM" NTRU CRYPTOSYSTEMS TECHNICAL REPORT, REPORT 13, 'Online! 9 March 1999 (1999-03-09), pages 1-14, XP002288214 Retrieved from the Internet: URL:http://www.ntru.com/cryptolab/pdf/NTRU Tech013.pdf> 'retrieved on 2004-07-12! the whole document	